تشريع قانون يفرض على أي مؤسسة عامة او خاصة، وبغض النظر عن نوعها، فإن اي جهة تخزن البيانات الحساسة للمواطنين ورقيا او رقميا يجب ان يفرض عليها نوع من انواع التشفير والسياسات الأمنية، تتولى وزارة الاتصالات تحديد مستويات التشفير و طول المفتاح حسب حجم البيانات و نوعها، وتضع الجهة التشريعية الحد الأدنى من التشفير داخل النصوص القانونية.
قبل البدء في اقتراح طرق للتشفير وتعديل للنظام، يجب عمل تحليل و تخطيط للنظام القائم الحالي، و تصميم كافة العمليات التجارية و الادارية داخل الشركة من قبل محلل نظام، لمعرفة نقاط ضعف نظامهم و اماكن تخزين البيانات وطرق التعامل معها ومناولتها، ثم معرفة قدرة الشركة على الاستثمار المادي في تكنولوجيتها، ونهاية قائمة بمعدات الشركة وموظفيها.

ولأن قسم التسويق يتنقل خارج مقر الشركة فإننا ولطبيعة نشاطها ونشاط القسم نقترح:

1) سياسة امنية تغلق كل منافذ الجهاز و قارئة الاقراص على اجهزة الشركة المحمولة، لضمان عدم نسخ البيانات خارج الجهاز او اصابته بفيروس.
2) سياسة أمنية لا تسمح للجهاز بالعمل خارج ساعات الدوام، لضمان عدم سوء استعمال الموظف للنظام، ولضمان عدم سماح اللص بفتح حساب الموظف على مدى ال16 ساعة خارج الدوام وهذا يصعب في عملية الاختراق.
3) سياسة أمنية لا تسمح للموظف او غيره بالاتصال بشبكة الحاسوب المحمول، لضمان عدم اصابة جهاز الشركة بفيروس يقرصن او يشفر او يسرب البيانات الحساسة كما في نقطة 1 .
4) توفير جهاز انترنت خاص بحاسوب الشركة، لضمان عدم انتقال فيروس عبر الشبكة من جهاز الى جهاز.
5) اغلاق المنافذ و حجب الIP الغير محتاجة، لضمان عدم حصول اي مخترق على اتصال غير شرعي من الممكن له استغلاله في تنفيذ هجمات على الجهاز المحمول
6) استعمال نظام كيربيروس ، ونقل نظام الشركة على سحابة الشركة، مستضافة عند سحابة أزور الخاصة بمايكروسوفت لتوفيرهم لسياسة 0-ثقة، كما يوفرون ألية تخزين المفاتيح لتخزن على السحابة حالة الحاجة لاسترجاعها ،وبما ان الموظفين ينتقلون من مكان الى اخر فإن نظام كيربيروس للتحكم في الوصول مفيد ومناسب جداً لطريقة نشاط القسم وأهمية البيانات التي تخزنها الشركة.
7) توفير ألية تخزين مؤقتة محلية على الجهاز حال فشل نظام الانترنت، مع عمل بصمة رقمية لكل سجل، وفي حالة فشل النظام فإن نزاهة البيانات و ديمومة استمرار عمل نظام الشركة مهم جداً كذلك من الناحية الأمنية
8) تشفير القرص باستخدام BitLocker-FileVualt، الذين يوفران مفتاح بحجم 128 او 256بت، باستعمال خوارزمية AES لضمان عدم سرقة القرص مادياً و كشف بياناته وسوء استغلالها من قبل لصوص او اشخاص غير مخولين
9) تشفير الملفات المؤقتة FBE من نقطة 7، وتوفير ملفين وهميين يمثلان مفاتيح تشفير ليس لها علاقة بالجهاز ولا بياناته، وتوثيق ما اذا حاول المستعمل للجهاز استعمالهما لفك تشفير الملفات المخزنة مؤقتا على جهاز الشركة، نضمن بهذه الطريقة تضييع المزيد من وقت المخترق لحماية سرية المعلومات من الانكشاف ومن التعديل او التسريب من قبل الموظف.
10) استعمال برنامج HEXnode للتحكم في الاجهزة عن بعد بباقة Ultra التي تكلف 30 دينار عن كل جهاز، وبافتراض 50 جهاز للقسم فإن الشركة ستدفع 1400 دينار او 270$ كحد أقصى سنوياً، في مقابل الكثير من المزايا و التحكم بالنظام.

من الشركات التي تستطيع توفير عروض امنية للشركة: شركة HexNode ، الحصول على مراجعة من NISSA "الهيئة الوطنية لأمن وسلامة المعلومات" ، شركة أبعاد للحلول التقنية ، شركة تميز للإستشارات وحماية المعلومات.

تشفير الملف File-Based Encryption FBE		تشفير القرص Full-Disk Encryption FDE	
عيوب	مميزات	عيوب	مميزات
• قد يتسرب بعض الملفات الى اماكن غير مشفرة مثل temp او swap • الحاجة للحفاظ على مجموعة كبيرة من المفاتيح و كلمات السر	• سريع. • حالة الاختراق لا يمكن كشف كل البيانات.	• امكانية اجراء عملية تكسير كلمة السر. • استهلاكه لموارد الجهاز حسب حجم البيانات المتواجدة عليه.	• عدم القدرة على كشف بيانات القرص حالة سرقته مادياً وربطه بجهاز اخر.

حسب توصياتي ال10 كخبير أمن معلومات أنفاً فإن نظام التشغيل لا يهم كثيراً، لإستخدامنا لسحابة مايكروسوفت أزور لتخزين نظام الشركة وملفاتها ومفاتيحها سحابياً ،مع نظام كيربيروس للتحكم في الوصول الغير مركزي. هذا يسمح لنا بالعمل مستقلين عن انظمة التشغيل و تفاصيلها وعيوبها.